(12) UK Patent Application (19) GB (11) 2 174 039 A

(43) Application published 29 Oct 1986

(21) Application No 8609030

(22) Date of filing 14 Apr 1986

(30) Priority data

(31) 724372 (32) 17 Aug 1985 (33) US
762994 6 Aug 1985
832802 25 Feb 1986

(71) Applicant
Pitney Bowes Inc. (USA-Delaware),
Walter H. Wheeler Jr Drive, Stamford, Connecticut 06926,
United States of America

(72) Inventors
George B. Edelmann,
Arno Muller,
Guy L. Fougere,
Kevin D. Hunter,
Ronald P. Sansone,
Alfred C. Schmidt Jr

(74) Agent and/or Address for Service
D. Young & Co., 10 Staple Inn, London WC1V 7RD

(51) INT CL⁴
G07B 17/04

(52) Domestic classification (Edition H):
B6F 233 262 A
B6C 1200 VSA
G4M A1 A2 A3 A4 B4 D6 F2 F4 P4 R6 T1 T2 TX U1 U6
U1S 2133 2268 B6C B6F G4M

(56) Documents cited
GB 1486596 GB 0939233
GB 0952211 EP A 0131964

(58) Field of search
B6F
B6C
G4R
Selected US specifications from IPC sub-class G07B

(54) Postage and mailing information applying system

(57) A postage and mailing information system wherein an encrypted message based upon postage and mail address information is created, this encrypted message being used in the determination of authenticity. By placing the encrypted message in the address field of a mail piece, authentication by an automatic high speed sorter is possible. The conventional franking indicia on the upper right corner of the mail piece is not therefore needed. The value of the postage and a customer code can be provided as the first line 38 of an address label 36; date, time and class of postage in second line 40; an encryption message, unique to that mail piece 34, is provided on a third line 42. These non-address lines can be bar-coded.

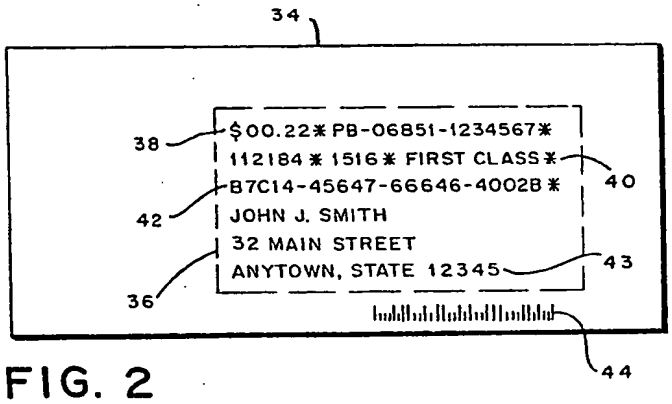


FIG. 2

GB 2 174 039 A

The drawings originally filed were informal and the print here reproduced is taken from a later filed formal copy.

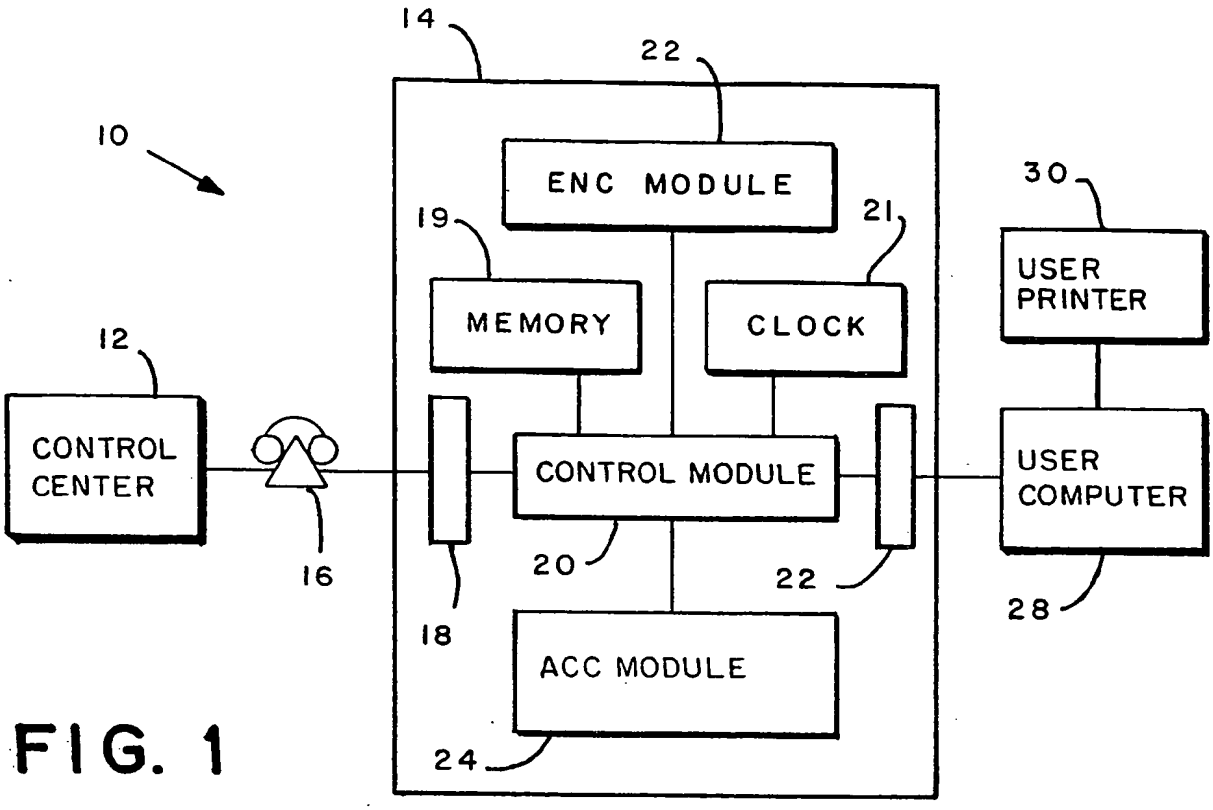


FIG. 1

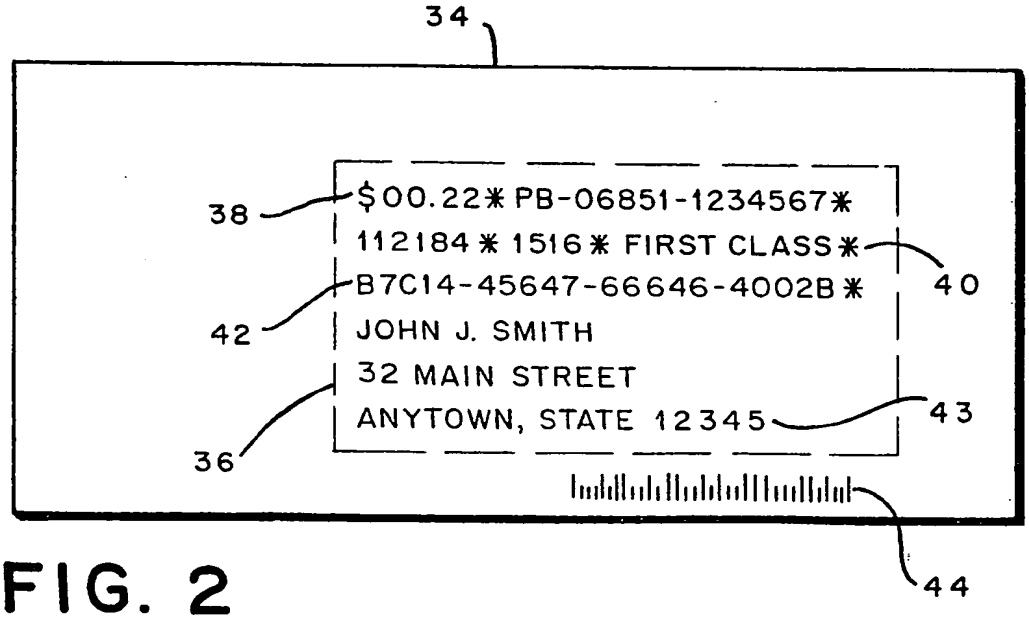


FIG. 2

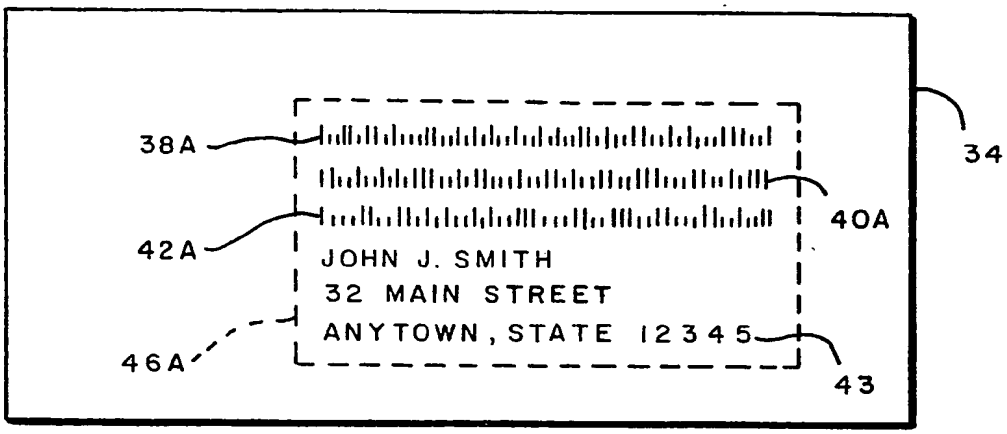


FIG. 3

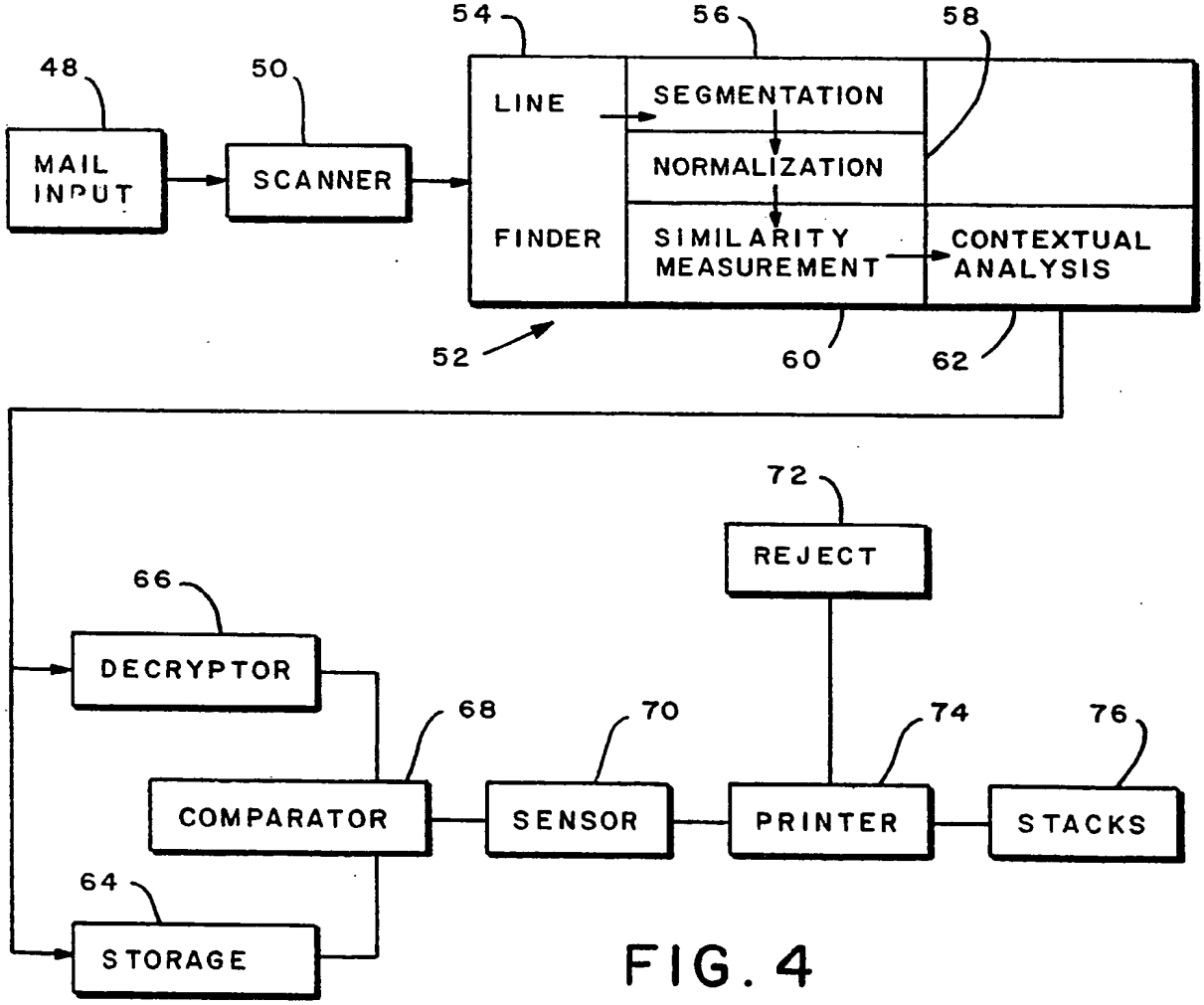


FIG. 4

FIG. 5A

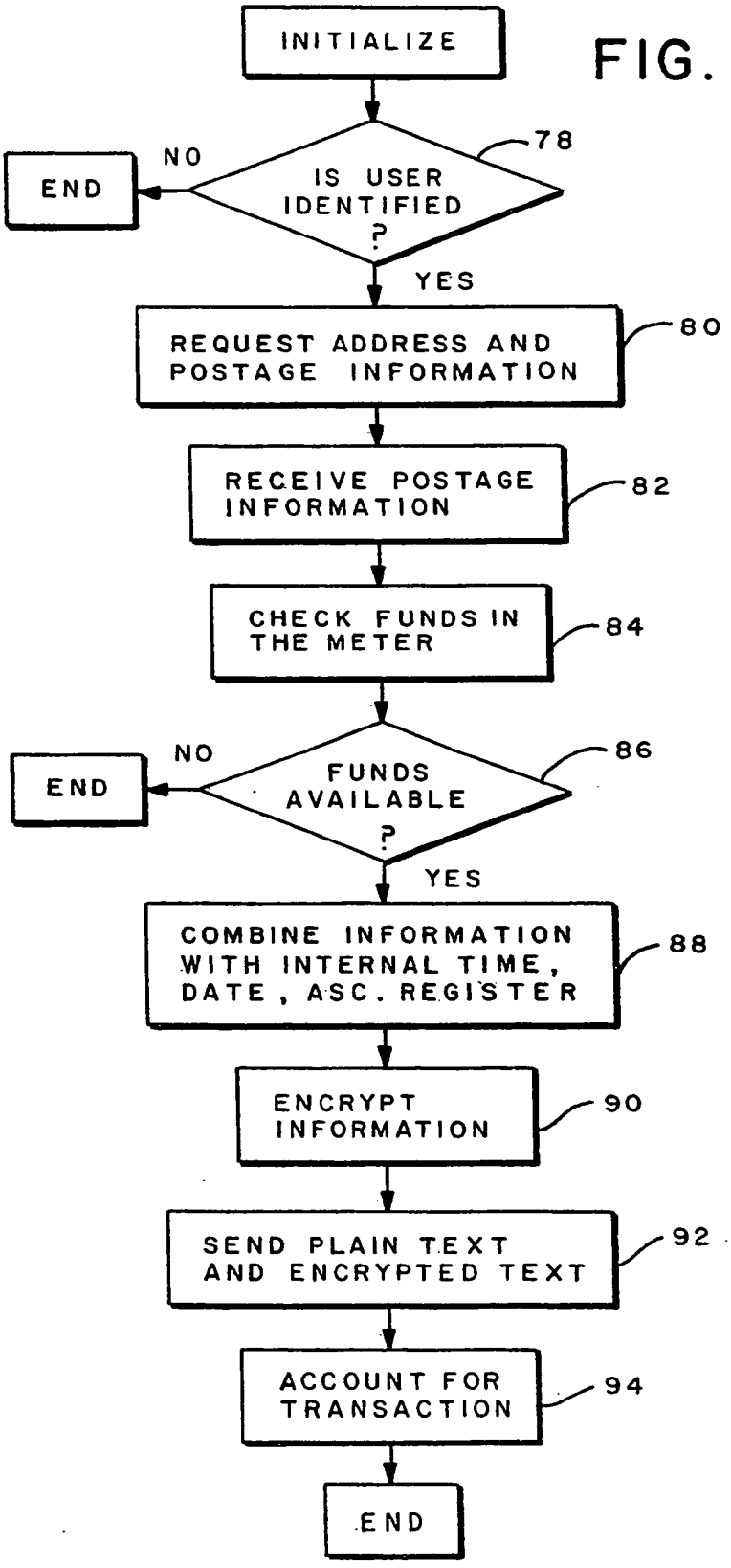


FIG. 5B

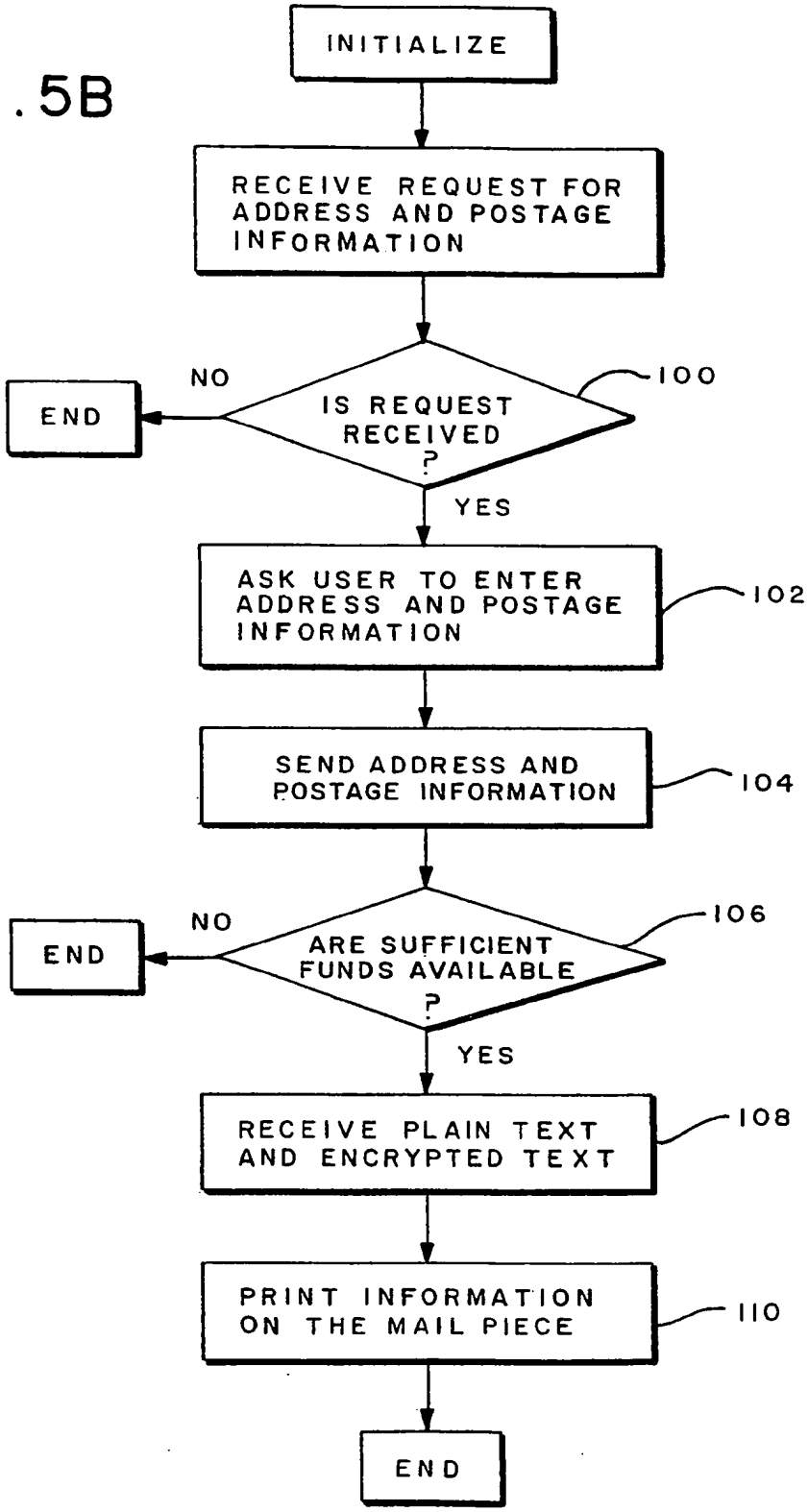
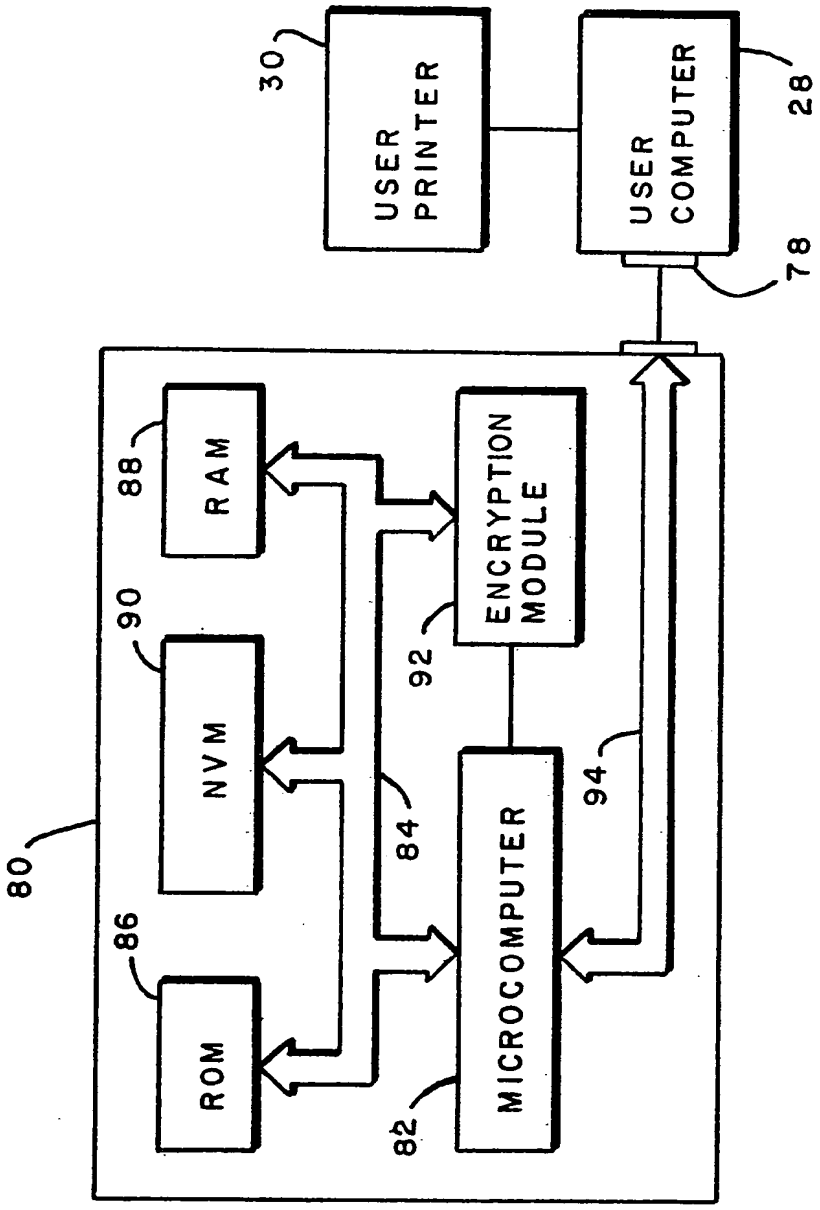


FIG. 6



SPECIFICATION

Postage and mailing information applying system

Since the issuance of U.S. Patent No. 1,530,852 to Arthur H. Pitney, March 24th 1925, the postage meter has had a steady evolution. Postage meters are mass produced devices for printing a defined unit value for governmental or private carrier delivery of parcels and envelopes. The term postage meter also includes other like devices which provide unit value printing such as a tax stamp meter. Postage meters include internal accounting devices which account for postage value, which postage value is stored within the meter. The accounting device accounts for both the recharging of the meter with additional postage value and the printing of postage by the meter printing mechanism. No external independent accounting system is available for accounting for the postage printed by the meter. Accordingly, postage meters must possess high reliability to avoid the loss of user or governmental funds.

Throughout the years, two general types of postage meters have been used: one that uses a rotatable print drum and is referred to as a rotary postage meter, and the other that uses a stationary print head and a reciprocating platen and is referred to as a flat bed postage meter. Most recently, there has been a change from a completely mechanical device to meters that incorporate electronic components extensively. Although there have been a number of changes, there are certain elements that remain constant. For example, the need for security is absolute. In prior postage meters, such security is applied both to the printing portion of the meter and to the accounting portion. The reason for the absolute security requirement is because a postage meter is printing value, and unless security measures are taken, one would be able to print unauthorized postage, thereby defrauding the U.S. Postal Service. Most security measures taken are of a physical nature, but recently there have been suggestions for the use of encryption to ensure that a postage indicia is valid. Nevertheless, such encryption merely supplements the physical security systems that have been used and suggested by the prior art. Furthermore, the known prior encryption systems attest to the validity of the indicia but provide no means for determining whether the printed indicia is just a copy of a valid indicia. Additionally, prior systems relied upon the post office accounting for postage by monitoring the number and value of mail pieces sent by a particular meter user.

Another common factor in prior postage systems is the inclusion of a postage indicia normally placed in the upper right hand corner of one surface of an envelope or package. This indicia has taken a specific form. The postage amount is contained in a rectangular border and the date of the postage impression appears in a circular border. This form has evolved from the original appearance of a canceled stamp wherein the stamp is of a rectangular configuration and the cancellation mark included the date within a circle. Also included in this indicia is the postage meter number and the city and state from which the envelope was mailed.

Although postage meters have performed satisfactorily in the past and continue to perform satisfactorily, with the advance of electronics, postage systems are needed that are less expensive and more flexible while still providing the serviceability and security required. Additionally, it would be desirable to have a postage system that is more compatible with contemporary mail processing systems.

Encryption is utilized to prevent fraudulent postage taking. An encryption message is derived from postage information and/ or recipient address information and applied to a mail piece. With the inclusion of recipient address information in the encryption message, there is a relationship between authentication and the mail piece that is unique for each mail piece. In accordance with one aspect of the instant invention, the postage information and encryption are placed in the address field of the mail piece along with address information. With the encryption in the address field, authentication can be made on the fly by an automatic mail scanning/sorting machine quickly and efficiently.

The invention is defined in the claims herein.

The invention will be better understood from the following non-limiting description of examples thereof given with reference to the accompanying drawings in which:-

Figure 1 shows a block diagram of a system that utilizes the invention;

Figure 2 is a plan view of a mail piece (an envelope) having postage information printed thereon in the address field in accordance with the invention;

Figure 3a is a view similar to Figure 2 but with bar codes instead of alphanumeric characters in a portion of the address field;

Figure 3b is a view similar to Figure 3a but showing a different format;

Figure 4 is a block diagram of a mail scanning/ sorting machine that can operate a method according to the invention;

Figure 5 is a flow chart showing cooperation between two components shown in Figure 2; and

Figure 6 is a block diagram of an alternative embodiment of the invention.

Referring initially to Figure 1, a postage and mailing information applying system is shown generally at 10 and includes a control center 12 and an accounting unit 14 that are in communication with one another through a communicating device such as a telephone 16, facsimile machine, telex machine, and the like.

Located within the accounting unit 14 is a modem or converter 18 which provides communication between the telephone 16 and a control module 20 of the accounting unit, which control module may be a CPU such as an Intel 8085 microprocessor available from Intel Corporation, Santa Clara, California. The control module 20 has a

memory 19 and a clock 21 either integral or in connection therewith. The memory 19 would store the transaction number, i.e. a number assigned to the accounting unit of the occasion of clarifying postage to the system 10, the customer number and the like. In communication with the control module 20 is an encryption module 22 as well as an accounting module 24. The encryption module would be any of a readily available encryption device which may, for example, encrypt in accordance with the NBS Data Encryption Standard (DES) pursuant to a preset secure key. An example of a suitable encryption module 22 would be an Intel 8294 encryptor. The accounting module 24 may be a battery augmented RAM that incorporates the ascending and descending registers. As is known from previous postage metering devices, the ascending register is the register that records the amount of postage that is dispensed or printed on each transaction and the descending register is the register that records the value, or amount, of postage that may be dispensed and decreases from an original or charged amount as postage is printed. Another modem 26 within the accounting unit 14 provides communication between the control module 20 and a user computer 28. The user computer may be any typical computer that has input, logic and output for example, a personal computer such as the IBM AT available from IBM Corp., Armonk, N.Y. Connected to the user computer 28 is a user printer 30. Although the user printer may be of any type that is capable of printing individual alpha numerics, a dot matrix printer is preferable since a dot matrix printer is capable of printing any configuration including bar codes.

In the block diagram shown in Figure 1, the control center 12 may be a Post Office which serves as a source of postage value. Systems are known whereby a postage meter may be charged remotely upon a user providing his assigned customer number to the Post Office, see for example U.S. Pat. No. 4,097,923. The Post Office, in turn, will provide postage value that is automatically input to the customer's postage meter, in this case the accounting unit 14. The postage value will be received within the descending register portion of the accounting module 24 to increase the amount to a figure that is the sum of that amount being charged and the unused amount from previous charging. In the system of Figure 1, the secure portion of the postage meter is replaced by the accounting unit 14 that is a secure unit such that tampering by physical, electronic or magnetic means is inhibited. Security features such as shields, break away bolts and the like are well known and the means for securing the accounting unit 14 will not be further described. In a preferred embodiment, the accounting unit 14 would have no display and would only be accessible by the user computer 28 upon an assigned code word being received by the control module 20 of this accounting unit 14 from the user computer. It will be understood that the user printer 30 is not a secure printer nor are the links between the user computer 28 and the accounting unit 14 and the user computer and the user printer. The postage information to be printed by the user printer 30 would include an encryption number that is generated by the encryption module 22. Encryption may be based upon any recognized code such as DES, supra, National Security Agency (NSA) cipher or Rivest, Shamir and Adleman (RSA) cipher. Upon the appropriate information being supplied to the accounting unit 14 from the user computer 28, the encryption module 22 would generate an encryption number which would then be communicated through the user computer 28 and printed by the user printer 30. This supplied information could include, the customer number, the value of postage and the like. In a particular embodiment of this invention, the street address, zip code and the like of the recipient is included in the encryption for the purposes of authentication. As used in this disclosure, authentication is defined as the determining of the genuineness of postage printed upon a mail piece.

Referring now to Figure 2, a format is shown for applying postage information and mailing information to the address field of a mail piece such as an envelope 34. By postage information is meant postage amount, date of mailing, meter or customer number, transaction number, class of mail and the like. By address information is meant the house number, name, city, state, zip code and the like of the mail recipient. In this particular configuration, an envelope 34 is shown with a label 36 attached in the address field portion of the envelope. As used in this specification and claims, the term address field has the meaning as defined in U.S. Postal Service regulations. Such definition may be found in the U.S. Postal Service's phamplet "Guide to Business Mail Properties", page 20, September, 1984. Although this embodiment is described with the combination of a label 36 and envelope 34, it will be appreciated that the characters may be printed directly upon the envelope or upon an insert that would be placed within a window type envelope. It will be understood that this label 36 replaces and eliminates the need for the normal indicia that is applied to the upper right hand corner of a mailpiece. One of the features of the instant invention is that a standard indicia is no longer required because the security features provided by such standard indicia are replaced by the security offered by encryption.

In a preferred embodiment, the first line 38 of the label would have information relative to the amount of postage and the customer number. The second line 40 contains the date of the mailing, the time the postage is imprinted and the class of mail. The third line 42 contains an encryption message in the form of numbers and letters that may be derived from the information on the first two lines as well as information from the address of the recipient of the mail piece that follows this third line. As shown, the printed lines are parallel to one another to facilitate automatic reading. It will be appreciated that other conventional machine readable configurations may be used rather than parallel lines.

The postage amount, customer number, date and class of mail are input through the keyboard of the user computer 28 to the control module 20. The encrypting module 22 then generates an encryption number or message and upon the print command being given by the computer operator, the time is determined and an encrypted message is obtained. This encryption message 42, is then printed by the user printer 30 on line 3 of the label 36. With this information, a Postal Service representative would be able to input the encryption message into a suitable computer and determine whether the postage is genuine by decrypting the information.

Although the system has been shown using alpha-numerics in the address field, it will be appreciated that bar code may be used to print the first three lines as shown in Figure 3. This bar code may be of any form including the bar-half bar configuration used presently by the Postal Service. The bar codes could be combined in an indicia for aesthetic purposes-and placed within the address field as shown in Figure 3b or in the upper right hand corner of the envelope 34. Although the bar code is shown extending parallel to the alpha-numerics, it will be appreciated that the bar codes could extend parallel thereto. The bar code also may appear on the bottom edge of the envelope as shown at 44 so as to be read by present Postal Service equipment.

The advantage of the system shown and described is that one is able to eliminate the standard postage indicia that has been in practice for decades and still provide the assurance associated therewith. In addition, by having all the information in the address field, authentication may be obtained quickly from information appearing on the envelope. Because of the presence of the recipient's zip code, the encryption message 42 that appears on the label 36 is unique for that mail piece. More specifically, there is a connection between the mail piece and the encryption message. In prior systems, there was no relationship between the code or encryption and the mail piece, but rather a seed number or the like was used in conjunction with sender information such as the sender's zip code, meter number, and the like. Present high speed automatic scanning/sorting machines incorporate OCR readers capable of reading the information in the address field of an envelope 34 and sorting in accordance therewith. An example of such an automatic scanning/sorting machine is the Pitney Bowes Optical Character Reader described in publication 150 of the United States Postal Service entitled "Automatic Mechanization for Mail Processing Systems", page 14, May, 1985. A decryption module could be added to such an automatic sorting machine by which the encrypted line 42 would be read as well as the address line by the OCR reader. This encryption module would determine the authenticity of the postage not only on the basis of the visual tests, postage, date, meter number and the like, but on the basis of the recipient address. In this manner, not only is a check made for authenticity of the postage but also for the fact that the encrypted line belongs to that particular piece of mail and only that piece because of the recipient address. More specifically, what is contemplated is a two way encryption scheme where the decryptor has a "key" to determine authenticity based upon information on the face of the envelope 34. This is in contrast to a two way scheme where seed numbers are used and encryption is performed twice and compared.

Referring now to Figure 4, such as automatic scanning/sorting machine with deciphering capability is shown. The machine includes a mechanical transport unit 48 that singulates batches of mail into a stream of mail pieces that are conveyed with a predetermined separation past the various stations of the machine including a scanner 50, a line finder 54, a segmentation block 56, a normalizer 58, a simularity measurer 60 and a contextual anaylsis block 62. Each envelope 34 is conveyed past the scanner 50 which produces digitized binary images of the address field consisting of black and white pixels. The line finder 54 finds the lines in the address field which are to be read. The segmentation module 56 separates the lines into characters. The normalization block 58 transforms the segmented characters into a predetermined size. The standardized character images are then transferred to a similarity measurement block 60 where they are compared against stored known character templats to obtain character recognition. The results of these comparisons are sent to the contextual analysis unit 62 where the final decision is made for the address portion of the information while the encryption portion passes through. An ASCII code representation of the recognized characters is then sent to both a buffer 64 that simply stores the address information and to a decipher 66 that decrypts the encryption line 42. The information from the buffer 64 and decipher 66 is then sent to a computer 68 where the information from each is compared. The results of the comparison are sent to a censor 70 where a determination is made as to the authenticity of the postage on the mail piece. If it is found to be authentic, the envelope 34 is routed to a sorting stack module 72, but if it is deemed to be fradulent, this envelope is sent to a rejection bin 74. In this way, genuineness of the postage on an envelope can be determined on the fly. Obviously, this process is enhanced because the printed information on the envelope 32 is applied in a parallel fashion thereby facilitating fast, automatic processing. If authentication is made, the encryption message may be printed in bar code form at the bottom edge of the envelope 32 as is now done with the address information by a bar code printer 76 of an automatic mail sorter. It will be understood that this bottom edge bar printing of the encrypted message may be performed alternatively by the user's printer 30 upon its being programmed to do so.

Referring now to Figure 5, a flow chart is shown wherein the cooperation between the accounting unit 14 and the user computer 28 is shown. The system is initialized 76 and a request is made 78 by the accounting unit 14 as to whether the user is

properly identified. If the user is identified, a request is made by the accounting unit 14 for address and postage information 80 for the purpose of generating the encryption message. The information is received 82 and a check for funds is requested 84. A determination is made if funds are available 86 and if sufficient funds are available, the information is combined 88 with the internal time, date, ascending registers and the other information in the accounting unit 14. The encryption message is generated 90 and the plain text and encrypted text are sent 92 to the user computer 28. As the plain text and encrypted text are sent, the transaction is accounted for 94 and the system is returned to its starting point. On the other hand, if funds are not available 86, then a message is sent to the user computer 28 that there are insufficient funds.

The user computer 28 initially receives the request from the accounting module 14 for the address and postage information 10. With this request, the user would enter the appropriate address and postage information 102 and this would be sent 104 to the accounting unit 14. After the address and postage information are conveyed, the question is asked whether sufficient funds were received 106. If sufficient funds were received, then the plain text and encrypted text are received 108 from the accounting unit 14 and the command is given 110 to print the information on a mail piece 34.

The instant invention has thus far been described with reference to an accounting unit 14 that communicates with a control center 12 through a telephone 16 and with a user computer 28. An alternative embodiment of the invention includes the use of a portable or removable data device in place of the accounting unit 14.

Reference is now made to Figure 6 wherein a system is described in which data may be input into the user computer 28 without contacting the central station 12 or accounting unit 14. In this system, the user computer includes an input port 78 adapted to received and provide communication with a removable data device 80. The removable data device 80 can be in the format of a "smart credit card" or a larger enclosed structure such as a cartridge or vault, and the like, which for purposes of this description and accompanying claims will be referred to collectively as a "card". The card 80, which appears enlarged in Figure 6 for descriptive purposes, provides physical support for and protection of a microcomputer 82 which is connected by a private bus 84 to a plurality of internal components. The microcomputer 82 is connected via the bus 84 to a read only memory (ROM) 86 which contains the operating program for the microcomputer 82. The program resident in the ROM 86 not only controls the operation of the microcomputer 82 but also provides operating instructions by which the microcomputer 82 communicates with the user computer 28.

The microcomputer 82 also is connected via the bus 84 to a random access memory (RAM) 88, or other operating memory, to provide dynamic data storage during operation. A nonvolatile memory (NVM) 80 such as an electrically erasable programmable read only memory (EEPROM) provides nonvolatile storage for encryption data. The NVM 80 may include descending register value, the ascending register value, piece count value and the like as well as address information. Any accounting or other data desired to be retained during power failure, such as during servicing, can also be filed in the nonvolatile memory 90. The nonvolatile memory 90 also may contain a user identification number, as well as various configuration data so that the user computer 28 is operable in various countries which have different requirements and in various systems which have different configurations. The microcomputer 82 is connected via the bus 84 to an encryption module 92 that performs the same functions as those described in connection with the encryption module 22.

In contrast to the private bus 94, which is not accessible by any user or by equipment external to the card 80, a public bus 94 is provided for communication with the user computer 28 and the card 80. It should be recognized that other devices peripheral to the user computer 28 can be connected to the public bus 94 such as additional printers, displays, communications devices and the like. The public bus 94 is a general purpose bus to allow communications between the user computer 28 and the components within the card 80 and between the card 80 and the central station 14 when the card is inserted within to input port 78.

It should be recognized that the user computer 28 is powered by an external source of power, not shown, and during normal operation provides the power to energize the microcomputer 82 as well as the various components of the card 80 including the ROM 86, RAM 88, NVM 90, and encryption module 92 via the bus 94. Power sensing circuitry, not shown, such as is disclosed in U.S. Pat. No. 4,285,050 for ELECTRONIC POSTAGE METER OPERATING VOLTAGE VARIATION SENSING SYSTEM, can sense the presence of falling power and cause the microcomputer 82 to invoke a power down subroutine stored in the ROM 86 to complete operations in progress and store accounting data into the NVM 90.

In essence, upon insertion within the input port 78, the card 80 would replace the accounting unit 14 to perform the same functions as required. Postage value may be supplied to the NVM 90 of the card through communication with the control center 12. This communication would be through the public bus 94. Under command of the microprocessor 52, information may be provided by the user computer 28 through the CRT and keyboard of the user computer. With the card 80 inserted into the port 78, all functions to the accounting unit 14 would be carried out by the card 80.

The address information, postage amount, user identification number, date and class of mail are input through the keyboard of the user computer 28 to the microcomputer 82. The encryption module S0 then generates an encryption number or message based upon such input and stored en-

crypted routines and upon the print command being given by the computer operator, an encrypted message is transmitted to the user computer 28. This encryption message 42, is then printed by the user printer 30 on line 3 of the label 36. With this information, a Postal Service representative would be able to input the encryption message into a suitable computer and determine whether the postage is genuine by decrypting the information as discussed previously.

CLAIMS

1. A mail piece containing thereon recipient mailing address information and encryption information derived from said recipient mailing address information.

2. A mail piece containing thereon postage information, recipient mailing address information and encryption information derived from said postage information and recipient mailing address information.

3. The mail piece of claim 2 wherein said encryption information is in bar code form.

4. The mail piece of claim 3 wherein the encryption information appears on the edge of said mail piece.

5. The mail piece of claim 2 wherein said information appears in the address field of the mail piece.

6. The mail piece of claim 2 wherein said information appears in alphanumeric form.

7. A mail piece containing a plurality of substantially parallel printed lines thereon, at least one of said lines containing postage information, at least one of said lines containing recipient address information and at least one of said lines containing encryption information derived from at least one of said lines containing postage information and recipient address information.

8. The mail piece of claim 7 wherein said encryption information line is in bar code form.

9. The mail piece of claim 7 wherein the encryption information line appears on the edge of the mail piece.

10. The mail piece of claim 7 wherein said lines appear in the address field of the mail piece.

11. A mail piece containing a plurality of machine readable lines thereon, at least one of said lines containing postage information, at least one of said lines containing recipient address information and at least one of said lines containing encryption information.

12. The mail piece of claim 11 wherein at least said encryption information line is in the form of bar code.

13. The mail piece of claim 11 wherein said lines appear in the address field of the envelope.

14. A method of applying postage and mailing information upon a mail piece, comprising the steps of:

applying upon a mail piece at least one line that contains postage information;

applying upon the mail piece at least one line containing recipient address information in parallel with said at least one postage information line;

applying upon the mail piece at least one line containing an encrypted message which is parallel to said postage information and recipient address information lines.

15. The method of claim 14 wherein the lines are applied within the address field of the mail piece.

16. The method of claim 14 including the steps of conveying the envelope through an automatic sorting machine containing an OCR reader module and an decryption module, reading the lines in the address field of the mail piece, decrypting the encrypted information and authenticating the postage applied to the mail piece.

17. The method of claim 14 including the step of printing a bar code representation of the encrypted message along one edge of the mail piece.

18. A method of placing an encryption message upon a mail piece, comprising:

communicating recipient address information to an encryptor,

communicating postage information to the encryptor,

deriving an encryption message based upon the communicated recipient address information and the postage information, and

placing the encryption message on the mail piece.

19. The method of claim 18 including communicating the recipient address zip code to the encryptor.

20. The method of claim 19 including communicating a mail sender identification number to the encryptor.

21. The method of claim 18 including printing the encryption message onto a label and attaching the label to a mail piece.

22. A method of placing an encryption message upon a mail piece, comprising:

communicating address information to an encryptor,

deriving an encryption message based upon the communicated address information, and

placing the encrypted message on the mail piece.

23. The method of claim 22 including communicating the mail address zip code to the encryptor.

24. The method of claim 23 including communicating a street address of the recipient to the encryptor.

25. The method of claim 22 including printing the encryption message onto a label and attaching the label to a mail piece.

26. A method of placing an encryption message upon a mail piece, comprising the steps of:

inserting a card into a computer

communicating address information to an encryptor supported by the card,

deriving an encryption message based upon the communicated address information, and

placing the encrypted message on the mail piece.

27. The method of claim 26 including communicating the mail address zip code to the encryptor.

28. The method of claim 26 including communicating a street address of the recipient to the encryptor.

29. The method of claim 26 including printing the encryption message in dot matrix form onto a label and attaching the label to a mail piece.

30. Apparatus for providing self authentication of a mail piece, comprising:

encryption means operative to derive an encryption message based upon postage information and address information,

means for communicating recipient address information to said encryption means,

means for communicating postage information to said encryption means, and

means for placing onto a mail piece an encryption message generated by said encryption means.

31. Apparatus according to claim 30 including mail piece authentication means including:

means for decrypting said encryption message, and means for comparing the decryption with said postage information and said address information to determine the authenticity of said mail piece.

32. Apparatus according to claim 31 wherein said address information includes the zip code of the mail piece recipient.

33. Apparatus according to claim 31 wherein said postage information includes an identification number unique to the mail sender.

34. Apparatus according to claim 31 wherein said mailing information includes the house number of the mail piece recipient.

35. Apparatus for providing self authentication on a mail piece, comprising:

encryption means operative to derive an encrypted message based upon address information,

means for communicating recipient address information to said encryption means, and

means for placing onto a mail piece an encrypted message derived from said address information by said encryption means.

36. Apparatus according to claim 35 including mail piece authentication means including:

means for decrypting said encrypted message, and

means for comparing the decryption with said address information to determine the authenticity of said mail piece.

37. Apparatus according to claim 35 wherein said address information includes the zip code of the mail piece recipient.

38. Apparatus according to claim 36 wherein said address information includes the street address of the mail piece recipient.

39. A verification system for the processing of mail, comprising:

a card having a processor, an encryption module and a memory, a computer having means for outputting information, a communication link between said card and said computer, a first printer in communication with said computer, means for supplying mail pieces to said first printer, a second printer in communication with said computer and means for supplying a sheet to said second printer.

40. The system of claim 39 wherein said memory has a descending register for storing postage value.

41. The system of claim 40 wherein said memory is non-volatile and contains an identification number.

42. The system of claim 39 wherein said mail piece supplying means is an inserter operative to place inserts into mail pieces and convey the mail pieces to said first printer.

43. The system of claim 39 wherein said first printer is a dot matrix printer and including means for supplying labels to said first printer.

44. A system including a computer for providing self authentication on a mail piece, comprising:

a card

means for providing communication between said card and computer

encryption means supported by said card and operative to derive an encrypted message based upon address information,

means for communicating recipient address information to said encryption means, and

means for placing onto a mail piece an encrypted message derived from said address information by said encryption means.

45. The system of claim 44 including mail piece authentication means comprising:

means for decrypting said encrypted message, and

means for comparing the decryption with said address information to determine the authenticity of said mail piece.

46. The system of claim 45 wherein said address information includes the zip code of the mail piece recipient.

47. The system of claim 46 wherein said address information includes the street address of the mail piece recipient.

48. A verification system for processing mail, substantially as herein described with reference to and as illustrated in the accompanying drawings.

49. Any novel combination or sub-combination disclosed and/or illustrated herein.

Printed in the UK for HMSO, D8818935, 9/86, 7102.
Published by The Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.